UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,177	05/15/2006	Joachim Hagmeier	DE920030011US1	7861

25259   7590   05/06/2009
IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER
POPHAM, JEFFREY D

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
05/06/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

RSWIPLAW@us.ibm.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/564,177	HAGMEIER ET AL.
	Examiner	Art Unit
	JEFFREY D. POPHAM	2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2009*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-18 and 20* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-18 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☒ All   b)☐ Some * c)☐ None of:

   1.☒ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
      Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
      Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 1, 3-18, and 20 are pending.

Response to Arguments

1.   Applicant's arguments filed 1/28/2009 have been fully considered but they are not persuasive.

Applicants "submit that the assertion in the Office Action that authentication information <u>must</u> be used in an authentication process is incorrect." This being the case, one will readily note that the authentication information need not be used for anything. Therefore, the authentication information is meaningless in the scope of claim 1, since it need not be used in any authentication procedure. If this is the case, as Applicant appears to be arguing in submitting that the statement that "authentication information must be used in an authentication process" in incorrect, one will see that the authentication information can be any value whatsoever, as "authentication information" is as broad as "information" when it is not used for any authentication. Furthermore, referring to this information as "authentication information" makes the scope of the claims unclear, as Applicant is stating that there is authentication information (which must be used in some form of authentication procedure, or it would not be called authentication information) which need not be used for authentication. If Applicant intends for the "authentication information" of the claims to not be used in any authentication process, the claims need to be amended to represent such. However, the

Examiner has reviewed the specification as originally filed and cannot find basis

for authentication information sent from a client to a server that is not used in an

authentication process. It is noted that using authentication information in an

authentication process does not mean that the information is verified as

authentic, but rather, that the information is merely used, somehow, in the

authentication process. This use could be determining that the data is of an

incorrect format or is not authentic and rejecting it, determining that the data is

authentic, generating the data (such as generating a signature to be used in

authentication), or the like.

Applicant argues that Maurin does not teach inserting authentication

information into a cookie or a request header by the browser. As basis for this

argument, Applicant states that Maurin teaches adding a certificate to a header

by a machine other than the client computer. This may very well be the case, at

least in some embodiments, but previous claim 5 does not refer to any

"certificate". Previous claim 5 (and current claim 1) merely require that

"authentication information" is inserted into the request header by a client's

browser. This authentication information is much broader than a certificate.

Authentication information could be a password, a user name, a certificate, a

signature, a PIN, a challenge (or its corresponding response), personal

information about a user, authentication algorithm information, authentication

parameters, a cookie, or various other data that is within the broad scope of

"authentication information". Therefore, one will see that "authentication

information" need not be a certificate in the independent claims as they stand

amended.

Paragraph 26 of Maurin, for example, teaches that "When a user

reconnects to the site in question, the browser 5 sends the corresponding cookie

to the server machine 2b in an HTTP request header. The server machine 2b

uses the information in the cookie to configure itself based on the user 4 that is

calling it. The information in question is for example a piece of personal

information related to said user 4 such as a unique identifier, a response to a

questionnaire that the user has filled out on the site visited, or a date and time at

which certain pages have been read." This section clearly teaches the browser

of the client sending a cookie to the server in an HTTP request header, such

cookie comprising information that is personal to the user. This personal

information is clearly "authentication information" as it is personal to the user and

can be used to identify and authenticate the user's identity. Furthermore,

Paragraph 24 describes that cookies are sent to the browser of the client

machine for subsequent utilization. Paragraph 25 goes on to state that such

cookies comprise "Cookie 1", "Cookie 2", and "% CERT". Therefore, the

certificate is clearly provided to the client for subsequent utilization (such

utilization has already been described with respect to paragraph 26). This clearly

shows that, in at least one embodiment, Maurin teaches a browser of a client

inserting a certificate into a request header.

Applicant also argues that Buch cannot be combined with Maurin since

Buch uses a peer-to-peer environment, while Maurin uses a client-server

environment. First noted is that the instant application describes that a server

may reside on a client. Page 7, paragraph 25, for example, recites "That

component acts as a proxy server running on the same client 1 as the browser 2"

with apparent reference to a signature component as "That". One will clearly see

from this section of the instant application that a server is not inherently a

computer or machine that is separate and distinct from clients, but could rather

be a component of a client itself. Therefore, client-server communications could

very well occur between a client and another client. Furthermore, Buch,

paragraph 23, explicitly defines a SIP node as "a SIP application running on a

computing device, which may operate as a SIP client or a server." As should

now be clear, the SIP nodes of Buch can be clients and/or servers. Therefore,

communication between two SIP nodes could come in the form of client-client,

server-server, or client-server communications. For further clarification, one may

merely view the next paragraph (24) of Buch, stating that "As defined in SIP, the

SIP client 72 is also called a "user agent client" (UAC) as it creates a new

request, and the SIP client 86 is also called a "user agent server" (UAS) as it

generates a response 90 to a SIP request." As should be unambiguously clear,

the requesting entity of Buch can be a client and the entity receiving the request

can be a server.

Claim Objections

2.   Claims 1, 3-11, 16-18, and 20 are objected to because of the following

informalities:

- Claim 1 recites inserting client authentication information into a request header "independently of an authentication process used by a server", which does not make sense. This objection has already been discussed in the response to arguments above, in that the scope of the claim is unclear due to this limitation. As opposed to copying the above into this section, reference is made to the first paragraph of the response to arguments section above. This is also the case for the claims that depend from claim 1, independent claims 8, 16, 20, and the claims that depend therefrom.

- Claim 10 refers to "said HTTP-request header", however, no HTTP-request header has been discussed previously in the claim or those from which it depends. For purposes of prior art rejection, "said HTTP-request header" has been construed as "an HTTP-request header". Claim 14 has the same issue.

- Claim 18 refers to "a client certificate containing a client name and a private key". However, this does not appear to have basis in the application as originally filed. While the certificate may contain a public key, it does not contain a private key.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.   Claims 8-11 and 14 are rejected under 35 U.S.C. 112, second paragraph,

as being indefinite for failing to particularly point out and distinctly claim the

subject matter which applicant regards as the invention.

Claim 8 attempts to claim first receiving a request header <u>from a client</u> and

then inserting authentication information into the request header using the client's

browser. This cannot be, however, as the client must insert information into the

request header before sending it. This issue stems from the fact that the claim

was previously directed to a proxy setup, wherein the entity that would perform

the method of claim 8 is a separate and distinct entity from the client. This is

further shown in claim 9, stating that "said system can be a proxy server, a

gateway, or a tunnel", showing that the system performing the method is not the

client itself. It must be made clear in claim 8 that <u>either</u> the client or a proxy

server is generating the request header (or inserting information into it), as it

cannot be both as is currently stated. Claim 10 goes on to refer to the

authentication information being inserted into the header by an insertion

component. The insertion component of the instant application, however, is

described as being a proxy or on a proxy and not part of the client. This entire

set of claims is unclear in that the claims are directed to a method performed by

a single device, wherein the device is multiple devices, which makes no sense. If

Applicant intends for this set of claims to be directed to a method performed on a

client, it must be clearly claimed such that there is no proxy performing any of the

processing, and no sending of a header away from a device before the device

inserts information into the header. Claim 14 recites decrypting a header "with

said public key using a hash algorithm resulting in a hash value". This makes no

sense, as the decryption is <u>not</u> performed using a hash algorithm, but rather, the

decryption is performed in order to decrypt a hash that was previously generated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

4.   Claims 1, 3-5, 8-9, 11-17, and 20 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Maurin (U.S. Patent Application Publication

2002/0133700) in view of Buch (U.S. Patent Application Publication

2003/0217165).

Regarding Claim 1,

Maurin discloses method for authenticating clients in a client-

server environment, wherein the client-server environment uses a

communication protocol that allows extensions of a request header

without violating the communication protocol, wherein the method

comprises the steps of:

Generating a request header at a client computer

(Paragraphs 18-26);

Inserting client authentication information into the request

header at a client computer by a client browser, without violating

HTTP protocol, resulting in an extended request header

independently of an authentication process used by a server

(Paragraphs 18-26); and

Sending the extended request header to the server

(Paragraphs 18-26);

But does not explicitly disclose receiving information from t

he server if authentication has been successful or that the insertion

is performed without the server requesting authentication

information (though Maurin does appear as though it works this

way).

Buch, however, discloses inserting client authentication

information a request header at a client computer by a client

browser without a server requesting authentication information,

sending the extended header to the server, and receiving

information from the server if authentication has been successful

(Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have

been obvious to one of ordinary skill in the art at the time of

applicant's invention to incorporate the signature authentication

system of Buch into the authentication system of Maurin in order to

allow the system to verify authenticity of a client by both checking

that the client is authenticated by a certificate that is certified by a

trusted authority and by a signature that can be produced only by

the client's private key that corresponds to that client's certificate's

public key, thereby providing additional proof in authentication and

improving security of the system.

Regarding Claim 20,

Claim 20 is a computer program product claim that is

broader than method claim 1 and is rejected for the same reasons.

Regarding Claim 3,

Maurin as modified by Buch discloses the method of claim 1,

in addition, Buch discloses that the authentication information is

included in a first request header for establishing a session with the

server (Figures 6-7; and Paragraphs 53-54).

Regarding Claim 4,

Maurin as modified by Buch discloses the method of claim 1,

in addition, Maurin discloses that the authentication information

comprises a client certificate containing a client name and a client

public key (Paragraphs 18-28); and Buch discloses that the

authentication information comprises a client certificate containing a

client name and a client public key, and a digital signature which

has been generated over a hash value of the request header

including the client certificate using a client private key (Figures 6-7;

and Paragraphs 26-27, 39, 44, and 53-54).

Regarding Claim 5,

Maurin as modified by Buch discloses the method of claim 1,

in addition, Maurin discloses that the authentication information is

automatically inserted into the request header by the client browser

(Paragraphs 24-26).

Regarding Claim 8,

Maurin discloses method for authenticating clients in a client-

server environment, wherein the client-server environment uses a

communication protocol that allows extensions of a request header

without violating the communication protocol, wherein a system

establishes communication between a client and a server, wherein

the method comprises the steps of:

Receiving a request header from the client (Paragraphs 18-

26 and 32);

Inserting authentication information into the request header

at a client computer by a client browser, without violating HTTP

protocol, resulting in an extended request header independently of

an authentication process used by the server (Paragraphs 18-26

and 49-54); and

Sending the extended request header to the server

(Paragraphs 18-26 and 49-54);

But does not explicitly disclose receiving information from

the server if authentication has been successful or that the insertion

is performed without the server requesting authentication

information (though Maurin does appear as though it works this way).

Buch, however, discloses inserting client authentication information a request header at a client computer by a client browser without a server requesting authentication information, sending the extended header to the server, and receiving information from the server if authentication has been successful (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client is authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that client's certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Regarding Claim 9,

Maurin as modified by Buch discloses the method of claim 8, in addition, Maurin discloses that the system can be a proxy server, a gateway, or a tunnel (Paragraphs 13, 18-26 and 49-54).

Regarding Claim 11,

Maurin as modified by Buch discloses the method of claim 8,

in addition, Maurin discloses that the authentication information

comprises a client certificate containing a client name and a client

public key (Paragraphs 18-28); and Buch discloses that the

authentication information comprises a client certificate containing a

name and a public key of the client, and a digital signature which

has been generated over the whole request header including the

client certificate using a private key of the client (Figures 6-7; and

Paragraphs 26-27, 39, 44, and 53-54).

Regarding Claim 12,

Maurin discloses a method for authenticating clients in a

client-server environment, wherein the client-server environment

uses a communication protocol that allows extensions of a request

header without violating the communication protocol, wherein at a

server side the method comprises the steps of:

Receiving a client request header generated at a client

computer, the request header containing authentication information

inserted into the request header by the client computer at a client

browser, without violating HTTP protocol (Paragraphs 18-26); and

Validating the authentication information contained in the

request header by a server authentication component (Paragraphs

5 and 28);

But does not explicitly disclose providing information to a client if authentication has been successful.

Buch, however, discloses validating authentication information received in a request header and providing information to a client, if an authentication has been successful (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the signature authentication system of Buch into the authentication system of Maurin in order to allow the system to verify authenticity of a client by both checking that the client is authenticated by a certificate that is certified by a trusted authority and by a signature that can be produced only by the client's private key that corresponds to that client's certificate's public key, thereby providing additional proof in authentication and improving security of the system.

Regarding Claim 13,

Maurin as modified by Buch discloses the method of claim 12, in addition, Maurin discloses that the authentication information comprises a client certificate containing a name and a public key of the client (Paragraphs 18-28); and Buch discloses that the authentication information comprises a client certificate containing a name and a public key of the client, and a digital signature which has been generated over the whole request header content using a

private key (Figures 6-7; and Paragraphs 26-27, 39, 44, and 53-54).

Regarding Claim 14,

Maurin as modified by Buch discloses the method of claim 12, in addition, Maurin discloses that the request header is an HTTP-request header (Paragraphs 18-26); and Buch discloses that the server authentication component performs the steps of:

Accessing a public key contained in a client certificate (Paragraphs 18-28);

Decrypting a digital signature contained in a request header with the public key using a hash algorithm resulting in a hash value (Paragraphs 18-28);

Applying the same hash algorithm as used by the client to the request header (Paragraphs 18-28); and

Considering authentication as successful if both hash values match (Paragraphs 18-28).

Regarding Claim 15,

Maurin discloses server system for authenticating clients in a client-server environment, wherein the client-server environment uses a communication protocol that allows extensions of a request header without violating the communication protocol, wherein a client provides authentication information in the request header to a server system, wherein the server system comprising:

A server machine configured to receive the request header

(Figure 1);

An authentication component to operate on the server

machine and with functionality to read the authentication

information contained in the request header, and to validate the

authentication information (Paragraphs 5 and 18-28);

Wherein the request header is generated by the client and

the authentication information is inserted into the request header at

the client by a client browser, without violating HTTP protocol

(Paragraphs 18-28);

But does not explicitly disclose not requesting authentication

information (though Maurin does appear as though it works this

way).

Buch, however, discloses that the client request header was

sent with authentication information contained therein without the

server having requested the authentication information from the

client (Figures 6-7; and Paragraphs 44, 50, and 53-54). It would

have been obvious to one of ordinary skill in the art at the time of

applicant's invention to incorporate the signature authentication

system of Buch into the authentication system of Maurin in order to

allow the system to verify authenticity of a client by both checking

that the client is authenticated by a certificate that is certified by a

trusted authority and by a signature that can be produced only by

the client's private key that corresponds to that client's certificate's

public key, thereby providing additional proof in authentication and

improving security of the system.

Regarding Claim 16,

Maurin discloses client system to be authenticated by a

server system in a client-server environment, wherein the client-

server environment uses a communication protocol that allows

extensions of a request header without violating the communication

protocol, wherein the client system comprises:

A browser operating on a client computer (Paragraphs 18-

26); and

A component operating on the browser for inserting client

authentication information into the request header independently of

an authentication process used by the server and, without violating

HTTP protocol (Paragraphs 18-26);

But does not explicitly disclose that insertion is performed

without the server requesting authentication information (though

Maurin does appear as though it works this way).

Buch, however, discloses inserting client authentication

information into a request header without a server requesting

authentication information (Figures 6-7; and paragraphs 44, 50, and

53-54).). It would have been obvious to one of ordinary skill in the

art at the time of applicant's invention to incorporate the signature

authentication system of Buch into the authentication system of

Maurin in order to allow the system to verify authenticity of a client

by both checking that the client is authenticated by a certificate that

is certified by a trusted authority and by a signature that can be

produced only by the client's private key that corresponds to that

client's certificate's public key, thereby providing additional proof in

authentication and improving security of the system.

Regarding Claim 17,

Maurin as modified by Buch discloses the client system of

claim 16, in addition, Maurin discloses that the authentication

information comprises a client certificate containing a name and a

public key of the client (Paragraphs 18-28); and Buch discloses that

the authentication information comprises a client certificate

containing a name and a public key of the client, and a digital

signature which has been generated over a hash value of the

request header content using a private key of the client (Figures 6-

7; and Paragraphs 26-27, 39, 44, and 53-54).

5.   Claims 6-7, 10, and 18 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Maurin in view of Buch, further in view of Bishop (U.S. Patent

7,343,351).

Regarding Claim 6,

Maurin as modified by Buch does not explicitly disclose that the client browser receives the authentication information from a smart card via a smart card reader.

Bishop, however, discloses that the client browser receives the authentication information from a smart card via a smart card reader (Column 17, lines 27-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card of Bishop into the authentication system of Maurin as modified by Buch in order to provide a secure smart card that is dedicated to security procedures in order to sign data and create authentication information, thereby increasing security by making it more difficult for a malicious entity to steal data from such a secure smart card.

Regarding Claim 7,

Maurin as modified by Buch discloses the method of claim 1, in addition, Maurin discloses that the authentication information is automatically inserted into the request header (Paragraphs 18-26); but does not explicitly disclose that the authentication information is received from a smart card via a smart card reader.

Bishop, however, discloses that the authentication information is received from a smart card via a smart card reader (Column 17, lines 27-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to

incorporate the smart card of Bishop into the authentication system

of Maurin as modified by Buch in order to provide a secure smart

card that is dedicated to security procedures in order to sign data

and create authentication information, thereby increasing security

by making it more difficult for a malicious entity to steal data from

such a secure smart card.

Regarding Claim 10,

      Maurin as modified by Buch discloses the method of claim 8,

in addition, Maurin discloses that the authentication information is

automatically inserted into an HTTP-request header by an insertion

component (Paragraphs 18-26); but does not explicitly disclose that

the authentication information is received from a signature

component.

      Bishop, however, discloses that the authentication

information is received from a signature component (Column 17,

lines 27-64). It would have been obvious to one of ordinary skill in

the art at the time of applicant's invention to incorporate the smart

card of Bishop into the authentication system of Maurin as modified

by Buch in order to provide a secure smart card that is dedicated to

security procedures in order to sign data and create authentication

information, thereby increasing security by making it more difficult

for a malicious entity to steal data from such a secure smart card.

Regarding Claim 18,

Maurin as modified by Buch does not explicitly disclose a smart card reader; and a smart card with a security module containing a private key of the client and a client certificate containing a client name and a private key, wherein the smart card provides the client certificate together with a digital signature to an inserting component, wherein the digital signature is the result of an encryption of a hash value of the request header containing the client certificate by means of the private key.

Bishop, however, discloses a smart card reader; and a smart card with a security module containing a private key of the client and a client certificate containing a client name and a private key, wherein the smart card provides the client certificate together with a digital signature to an inserting component, wherein the digital signature is the result of an encryption of a hash value of the request header containing the client certificate by means of the private key (Column 17, lines 27-64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card of Bishop into the authentication system of Maurin as modified by Buch in order to provide a secure smart card that is dedicated to security procedures in order to sign data and create authentication information, thereby increasing security by making it more difficult for a malicious entity to steal data from such a secure smart card.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437